KnowBe4
PHISHING BY INDUSTRY BENCHMARKING REPORT

2024 EDITION

TABLE OF CONTENTS

According to **Verizon's 2024 Data Breach Investigations Report, human error was often a contributing factor to data breaches, playing a role in 68% of cases occurring through accidental actions**, the use of stolen credentials, social engineering and even through malicious privilege misuse. However, the report authors excluded privilege misuse from the calculation of the human element to better assess the impact of security awareness programs. Notably, the findings indicate that **the human element continues to play a significant role**, indicating that mitigating human-based risk should be a key priority for organizations.

INTRODUCTION

Cybercriminals can gain access to a digital environment in a variety of ways. As technical security controls continue to make "hacking in" increasingly difficult, cybercriminals look for less resilient targets: the human layer. As the human layer continues to be the most enticing attack vector, criminals are showing their willingness to search for any weakness, targeting employees in both professional and personal settings. Sadly, most organizations continue to focus on technology-based security layers while ignoring the human layer. Additionally, most humans remain vulnerable because they don't take precautions in their personal lives to prevent being compromised.

Cyber threats continue to grow as criminals rely on the tried and tested attack methods while developing new, more sophisticated ways to infiltrate digital environments and minimize the effectiveness of your human defense layer. To best defend your organization from a cyber attack, employees must have the knowledge, adapted habits and behaviors necessary to drive a culture of security. Training needs to be transformed into something more developed, consistent and instinctive.

We continue to see significant year-over-year increases in phishing attacks across all geographies, industry verticals and organization sizes. Cybercriminals do not discriminate when they consider victims, as carefully constructed attacks target humans both at work and play, day or night through various types of social engineering. Cybercriminals will continue to exploit humans as they determine their next intrusion strategy. As we continue to deal with socioeconomic and health issues globally, we also need to contend with advancements in artificial intelligence (AI) strengthening a cybercriminal's arsenal.

In 2023, the **FBI's Internet Crime Complaint Center (IC3)** reported an unprecedented surge in cyber crime incidents, **registering 880,418 complaints.** These complaints reflect an alarming potential for financial damage **with losses exceeding $12.5 billion. This is a nearly 10% increase in complaints received, and it represents a 22% increase in losses compared to 2022.**

Despite the daunting increase in reported cyber crime, the IC3 has seen measurable successes in tracking down and disrupting fraudulent schemes through collaboration with law enforcement agencies and advanced technology.

To address this challenge, a paradigm shift is necessary. Rather than viewing employees as inherent weaknesses, organizations should empower them as active participants in the fight against cyber crime. This can be achieved through the implementation of a proactive, comprehensive security awareness strategy that goes beyond mere compliance training. This new-school approach emphasizes continuous education, testing and communication to ensure that employees are equipped with the knowledge and skills needed to effectively combat evolving cyberthreats. As they launch more social engineering attacks, cybercriminals are betting that employees will lack the knowledge, attention and energy to thwart them. After all, one over-stressed, distracted, or uneducated employee is all it takes to let the bad actors in.

Security leaders need to know what happens when their employees receive phishing emails: are they likely to click the link? Get tricked into giving away credentials? Download a malware-laced attachment? Will they simply ignore the email or delete it without properly notifying their security team? Or will they report the suspected phish and play an active role in the human defense layer? By providing the knowledge, skills and tools they need to identify and respond to potential threats, organizations can transform their people from a liability into a powerful asset.

> Rather than **viewing employees as inherent weaknesses**, organizations should **empower them as active participants** in the fight against cyber crime.

UNDERSTANDING RISK BY INDUSTRY

The metric representing each organization's vulnerability to phishing attempts is termed Phish-prone Percentage (PPP). By expressing phishing susceptibility in quantifiable terms, leaders are empowered to assess their potential risk of a breach and implement targeted training to diminish their workforce's susceptibility to cyber threats.

An organization's PPP indicates the percentage of employees likely to fall for social engineering or phishing scams at any given time. As such, it is a good indicator of an organization's risk of and resilience against such attacks. These employees are the potential targets for social engineering attacks because they are susceptible to actions, such as clicking on malicious links, opening files laced with malware or unintentionally diverting company funds into accounts of cyber adversaries. By evaluating employee vulnerability to these actions, organizations can better understand their overall security posture and take appropriate measures to mitigate risks.

A high PPP indicates greater risk, as it points to a higher number of employees who are likely to fall for these scams. Conversely, a low PPP means that an organization's human layer of security is providing security strength rather than weakness. A low PPP is optimal, as it indicates the staff is security-savvy and understands how to recognize and shut down such attempts.

This overall PPP offers even more value when placed in context. After seeing their PPP, many leaders ask questions such as, "How does my organization compare to others?" and "What can we do to reduce our Phish-prone Percentage and better equip our team?"

To help organizations evaluate their PPP and understand the implications of their ranking, KnowBe4 conducts an annual study to provide Phish-prone benchmarking across industries. The research, organized by industry sector and company size, reveals patterns that provide insights into creating a stronger, more resilient cybersecurity culture.

2024 GLOBAL PHISHING BY INDUSTRY BENCHMARKING STUDY

While every organization aspires to gauge its performance relative to peers within its industry, achieving a meaningful comparison requires comprehensive data and the application of a scientifically validated approach to yield credible outcomes. For many organizations, "How do I stack up against similar organizations?" is a difficult question to answer.

That's where our annual Phishing by Industry Benchmark study comes in. To provide a nuanced and accurate answer, the 2024 study analyzed a data set covering over 54 million simulated phishing tests across more than 11.9 million users from 55,675 organizations in 19 different industries.

Methodology For This Year's Study

All organizations were categorized by industry type and size. Each organization's PPP was calculated by measuring the percentage of employees who clicked a simulated phishing link or opened a simulated malware attachment during a KnowBe4 testing campaign.

In our 2024 report, we continue to look at the following benchmark phases:

- **Phase One:** Baseline Phishing Security Test Results
- **Phase Two:** Phishing Security Test Results Within 90 Days of Training
- **Phase Three:** Phishing Security Test Results After One Year-Plus of Ongoing Training

ANALYZING TRAINING IMPACT

To understand the impact of security awareness training, we measured outcomes at these touchpoints to answer the following questions:

PHASE ONE

If you have not trained your users and you send a phishing attack, what is the initial resulting PPP?

To do this, we monitored employee susceptibility to an initial baseline simulated phishing security test. From that established set of users, we look at any time a user has failed a simulated phishing security test prior to having completed any training.

PHASE TWO

What is the resulting PPP after your users complete training and receive simulated phishing security tests within 90 days after training?

We answered this question by finding when users completed their first training event and looking for all simulated phishing security events up to 90 days after that training was completed.

PHASE THREE

What is the final resulting PPP after your users take ongoing training and monthly simulated phishing tests?

To answer this, we measured security awareness skills after 12 months or more of ongoing training and simulated phishing security tests, looked for users who completed training at least one year ago, and took the performance results on their very last phishing test.

METHODOLOGY AND DATA SET

54.1M Phishing Security Tests

11.9M Users

55.7K Organizations

19 INDUSTRIES

- Banking
- Business Services
- Construction
- Consulting
- Consumer Services
- Education
- Energy & Utilities
- Financial Services
- Government
- Healthcare & Pharmaceuticals
- Hospitality
- Insurance
- Legal
- Manufacturing
- Not For Profit
- Other
- Retail & Wholesale
- Technology
- Transportation

ORGANIZATION SIZE RANGES

42,488 Organizations	9,934 Organizations	3,253 Organizations
1-249	250-999	1000+

WHO'S AT RISK: RANKING INDUSTRY VULNERABILITY

The findings from the analysis of 11.9 million users underscore a widely recognized reality for organizations: inadequate user training results in both individual and organizational susceptibility to social engineering schemes. The PPP data from the initial phases revealed that organizations across all industries and sizes continued to face significant challenges in identifying and combating phishing attacks, with results showing a higher susceptibility compared to the previous year's findings. However, a marked improvement was noted during Phase 3, showing that when consistent and comprehensive training was applied for one year or more, there was greater preparedness against such threats. Yet, baseline security assessments performed without prior user training still revealed a significant vulnerability among workers to fall prey to phishing scams. That, in turn, could jeopardize their organizations with potential security breaches.

The results are unequivocal: systematic, continuous training is effective. Its positive impact is clear. Without robust training programs, users remain unprepared. The upturn in Phase 3 illustrates that when users are properly educated and tested, their ability to recognize and resist phishing and other social engineering tactics is enhanced, bolstering the overall security posture of their organizations.

The 2024 PPP Phase 1 (Baseline) statistics reveal an overall average susceptibility rate of 34.3% to phishing attempts across all industries and organizational sizes. That is an unwelcome uptick of just over one percentage point from the 2023 benchmark. This increase underscores the ongoing vulnerability in cyber defense readiness across different industries. Crucially, our research confirms that untrained employees remain the primary weak point in any organization's defense. Individuals lacking essential cybersecurity awareness, training and testing represent a significant vulnerability, leaving their organizations open to devastating cyber attacks. It's clear that empowering users with the knowledge and skills to detect and respond to cyber threats is an indispensable component of a robust security strategy.

Who's at Risk?

The top three riskiest industries by organization size

SMALL 1-249	MEDIUM 250-999	LARGE 1,000+
34.7% Healthcare & Pharmaceuticals	**39.7%** Hospitality	**51.4%** Healthcare & Pharmaceuticals
32.4% Education	**38.8%** Healthcare & Pharmaceuticals	**48.8%** Insurance
31.2% Hospitality	**36.2%** Consulting	**47.8%** Energy & Utilities

Following are the top three industries at highest risk in each organizational size category:

- Among small organizations (1-249 employees), the **Healthcare & Pharmaceuticals** industry lands in the top three for the third year, after spending the past two years at the number one spot, with a PPP of **34.7%**. This is a two-point backstep over previous results. Education also finds itself in the top three for the third year at the number two spot with a PPP of **32.4%**, slightly more than one point more lower than the prior year. New to the top three in 2024 is **Hospitality** with a PPP of **31.2%**, a setback of more than four points over the prior year. All leaders encountered a decline from their past positions.

- With mid-sized organizations (250-999 employees), the **Hospitality** industry moves into the top spot with a PPP of **39.7%**, an 11-point regression versus 2023. This marks Hospitality's second time in the leading position in the past three years. The **Healthcare & Pharmaceuticals** industry is in the top three for the third year. This year, it shifted down into the number two spot with a PPP of **38.8%**. Despite no longer occupying the top position, performance has still deteriorated by three points compared to last year. The **Consulting** industry is in the top three for the first time with a PPP of **36.2%**. That marks a five-point downturn from 2023. Each leader faced a downturn compared to their previous performance.

- For large organizations (1000+ employees), **Healthcare & Pharmaceuticals**, which achieved top-three rankings across all organizational sizes, secured the number one position with a PPP of **51.4%**. That reflects a nearly five-point deterioration from 2023. The Insurance industry has relinquished its two-year hold as the most at-risk sector. It moved to second place with a PPP of **48.8%**, a 4.5-point improvement over the prior year. The **Energy & Utilities** industry maintains its three-year streak in the top three, though it shifted from second to third with a PPP of **47.8%**. That represents just over a three-point improvement compared to 2023.

- The winner of the lowest PPP benchmark across small organizations (1-249 employees) was **Technology** with a PPP of **26.1%**; across mid-sized organizations was **Government** for the third year running with a PPP of **27.8%**; and across large organizations again for the third year we see **Government** with a PPP of **28.6%**. Despite each achieving the lowest PPP within their respective size categories, the results are less favorable across the board compared to previous data. This finding underscores that an untrained user base remains highly susceptible to phishing threats.

> "…the results are less favorable across the board compared to previous data.
>
> This finding underscores that **an untrained user base remains highly susceptible to phishing threats.**

BASELINE PHISHING SECURITY TEST RESULTS

As stated in the above methodology section, the initial baseline phishing security test was administered within organizations that had not conducted any security awareness training from the KnowBe4 platform. The tests were conducted without prior alerts, targeting individuals performing their routine work tasks without any specialized training. The results continue to indicate high risk levels year over year:

- Spanning every industry and organizational scale, the average PPP stood at 34.3%, one percentage point worse than 2023. This means that roughly one in three employees remained inclined to interact with malicious encounters, essentially mirroring the results from prior year.

- The 2024 data showed that although **Large Insurance** organizations are most at risk industries in the large category, the most significant improvement was seen with **Large Insurance** organizations, which saw a positive movement from a PPP of **53.2% in 2023 to 48.8% in 2024**. It may seem paradoxical to note that while they are one of the worst performing, they also exhibited the most improvement.

- The most significant decline was visible in **Medium Hospitality** organizations, which moved negatively from **28.5% in 2023 to 39.7% in 2024**, an 11-point regression. In 2023, the distinction went to Large Hospitality organizations. The Hospitality industry's role in amassing, handling and preserving vast quantities of customer information renders it a prime target for cybercriminals. Data managed within this industry (i.e., hotels, restaurants and casinos) often encompass extensive and sensitive personal data. The widespread global footprint of the industry provides an expansive attack surface, and it routinely employs a workforce that may have a lower level of cybersecurity preparedness.

- The most troubling results continue to be found in the **Large** category, where several industries have PPPs in excess of 40%: **Banking (42.3%), Consulting (47%), Energy & Utilities (47.8%), Financial Services (41.6%), Healthcare & Pharmaceuticals (51.4%), Insurance (48.8%) and Retail & Wholesale (42.4%)**. New to this list in 2024 are Financial Services and Retail & Wholesale. For the others, it's concerning to observe that for the third consecutive year, they have remained above a 40% PPP threshold, which indicates a high level of continued vulnerability.

Phase One

34.3%

Initial Baseline Phishing Security Test Results

Organization Size	Initial PPP
1-249	28.7%
250-999	31.9%
1000+	37.5%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	27.8%	33.3%	42.3%
Business Services	26.7%	31.6%	33.2%
Construction	28.8%	35.0%	32%
Consulting	28.4%	36.2%	47%
Consumer Services	28.8%	31.2%	31.6%
Education	32.4%	31.2%	31.7%
Energy & Utilities	29.3%	33.3%	47.8%
Financial Services	28.1%	31%	41.6%
Government	27.9%	27.8%	28.6%
Healthcare & Pharmaceuticals	34.7%	38.8%	51.4%
Hospitality	31.2%	39.7%	31.8%
Insurance	28.6%	34.1%	48.8%
Legal	26.5%	29.2%	35.2%
Manufacturing	27.9%	31.6%	35.9%
Not-For-Profit	30.3%	33.9%	36.7%
Other	26.3%	28.9%	29.7%
Retail & Wholesale	30.7%	32%	42.4%
Technology	26.1%	30.3%	32.9%
Transportation	27%	28.6%	35.1%

TAKEAWAYS

Organizations must prioritize and enhance their investment in the management of human risk. Merely paying lip service to security awareness programs does little to shield an organization from attacks that target human vulnerabilities.

Effective security education must be frequent, comprehensive and effectively executed. Training should not be a standalone effort; it must be woven into the very fabric of an organization. Additionally, it is vital to cultivate a security-conscious culture, where employees grasp the importance of safeguarding both their professional and personal environments. Employees must recognize their role in the company's cyber defense and be equipped with the knowledge to act accordingly. In this environment, security readiness becomes an integral part of the corporate ethos, fostering a workplace where vigilance and responsible behavior are instinctual and second nature to all.

Without ongoing training, regular testing, reinforcement and a strong cybersecurity culture, organizations of all sizes and industries remain vulnerable to phishing and other social engineering attacks. A skilled and vigilant workforce is essential to prevent infiltration, no matter how advanced or layered the technological defenses may be. To ensure comprehensive protection, organizations must stop relying on check-the-box security education and training for their employees. Instead, they need to invest in both robust security awareness programs and cutting-edge technological infrastructure. Security awareness training and testing needs to be offered with a high degree of quality and frequency and administered in the most efficient manner. Smaller bursts of content delivered more often keeps security top of mind and skills sharpened. Without training and frequent reinforcement, every organization, regardless of size and vertical, is susceptible to phishing and social engineering. Workforces represent a possible doorway to attackers, no matter how steep the investment in world-class security technologies. Investment in both training and technology provides the right mix of coverage.

PHISHING SECURITY TEST RESULTS WITHIN 90 DAYS OF TRAINING

Outcomes were significantly enhanced when organizations adopted an integrated approach of educational content along with simulated phishing tests following their initial benchmark evaluation. Our research revealed a marked improvement on simulated phishing assessments up to 90 days after initial training and testing. This improvement resulted in a reduction of nearly 50% in the average PPP, bringing it down to 18.9%, in line with trends observed over the past five years. Importantly, this decrease in vulnerability to phishing was not confined to particular industries or contingent on organization size.

- In **Small** organizations (1-249 employees), average outcomes aligned closely with the 2023 data, demonstrating a reduction of phishing susceptibility by approximately half over the prior year. Modest improvements were noticed within specific industries, while **Insurance, Technology and Transportation** showed signs of more substantial advancements.

- Similarly, with **Mid-sized** organizations (250-999 employees), all industries witnessed a significant reduction in phishing vulnerability after combining training and testing for 90 days. While this was a universal trend, the **Legal and Transportation** industries specifically exhibited moderate improvements, highlighting their positive progression.

- The trend persisted among **Large** organizations (1000+), with all industries experiencing a substantial reduction in phishing susceptibility after the 90 days of continuous and comprehensive training and simulated testing. The **Banking, Financial Services, Insurance and Retail & Wholesale** industries saw even greater results over prior year. This consistent decrease in phishing risks confirms the effectiveness of the measures employed, which have proven beneficial across all industries and organizational sizes.

Takeaways: Implementing just three months of new-school security awareness training can significantly improve employees' ability to identify suspicious emails, a trend observed across all industries and organization sizes. This 90-day investment proves to be a crucial and beneficial first step toward reducing human risk.

Transforming behavior requires persistence, as old habits must be broken to establish new, secure ones. As these new habits become more ingrained and instinctive, they evolve into standard practices that shape the organization's culture. This culture, in turn, guides the actions of current employees and serves as a reference point for new hires, who often look for cues on the social and cultural norms within the workplace.

Phase Two
18.9%
Phishing Security Test Results Within 90 Days of Training

Organization Size	90-Day PPP
1-249	19.9%
250-999	20.1%
1000+	18%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	13.9%	16.6%	13.8%
Business Services	20.8%	21.9%	21.3%
Construction	20.8%	21.5%	19.6%
Consulting	20%	21.8%	21.9%
Consumer Services	20.5%	20.9%	19.3%
Education	19%	19.4%	18%
Energy & Utilities	18.7%	19.5%	16.7%
Financial Services	17.4%	17.9%	18%
Government	17.7%	17.1%	15.6%
Healthcare & Pharmaceuticals	21.9%	20.8%	17.7%
Hospitality	21.9%	23.7%	15%
Insurance	20%	19.3%	15.7%
Legal	18.8%	16.7%	18%
Manufacturing	19.6%	19.8%	17.4%
Not-For-Profit	23.1%	23%	21.8%
Other	20.6%	21.5%	18.8%
Retail & Wholesale	20.6%	21.1%	18.3%
Technology	21.1%	20.8%	18.5%
Transportation	21.1%	20.4%	20.5%

PHISHING SECURITY TEST RESULTS AFTER ONE YEAR-PLUS OF ONGOING TRAINING

In this phase, we evaluate the efficacy of security awareness skills following 12 months or more of sustained training and simulated phishing evaluations. Our analysis includes individuals who concluded their training at least one year prior and reviews the performance results on their most recent phishing tests. The year-over-year findings are consistently impressive, reinforcing the impact of a steady, well-developed awareness training program. The new-school security awareness training has notably reduced the average PPP from **34.3% to just 4.6%**, with this significant decrease being evident uniformly across organizations of varying sizes and sectors.

For the fourth year, the lowest PPP in **Small** organizations (1-249 employees) was **Banking** at 2.3%. Given that the banking industry is among the most frequently targeted by cyber attacks and is subject to stringent regulations, the impressive results stem from the industry's extensive experience with cyber crime and the rigorous commitment it has made to security training. For **Midsize** organizations (250-999 employees), **Banking** takes the lead once more with a PPP of 3.3%. For **Large** organizations (1000+ employees), the **Hospitality** industry saw the lowest PPP at 3.4%.

After comparing the data, **Healthcare & Pharmaceuticals** is the industry that showed the greatest aggregate PPP improvement across small, mid-size and large organizations after 12 months of training and testing. This sector achieved an 88.8% reduction—moving from a benchmark PPP of 45.4% to 5.1% after 12 months of intervention. For the third year, **Energy & Utilities** went from a benchmark PPP of 41.6% to 3.98% after 12 months —a 90.4% reduction.

The **Healthcare & Pharmaceutical** industry remains a prime target for cybercriminals due to the vast amounts of sensitive patient data, outdated systems and lack of staff cyber preparedness. Successful attacks can compromise patient privacy, disrupt medical services and erode public trust. Similarly, the **Energy & Utility** sector is a key focus for cyber threats, particularly from nation-state actors seeking to disrupt security and economic stability. The industry's complex, geographically dispersed infrastructure creates a large attack surface, making it challenging to defend against sophisticated intrusions.

The growing adoption of AI in both industries presents risks if not implemented with strong cybersecurity measures. Adversaries may launch AI-driven attacks or exploit vulnerabilities in AI systems to further their malicious goals.

To mitigate these risks, **Healthcare** and **Energy** organizations must prioritize cybersecurity in their digital transformation plans. This includes investing in secure infrastructure, regularly updating systems and providing comprehensive employee training. Fostering a culture of cyber awareness and resilience is crucial to protecting critical assets, maintaining public trust and ensuring uninterrupted essential services.

Phase Three
4.6%
Phishing Security Test Results After One Year-Plus of Ongoing Training

Organization Size	12-Month PPP
1-249	4.3%
250-999	4.6%
1000+	4.9%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	2.5%	3.3%	5.2%
Business Services	5.3%	4.7%	5.3%
Construction	4%	4.8%	4.6%
Consulting	4%	4.6%	4.4%
Consumer Services	5%	5%	4.8%
Education	3.9%	5.2%	4.9%
Energy & Utilities	3.7%	4.2%	4%
Financial Services	3.5%	4.6%	4.7%
Government	4.4%	4.3%	4.5%
Healthcare & Pharmaceuticals	5.4%	4.3%	5.5%
Hospitality	4.2%	4.4%	3.4%
Insurance	3.8%	5.2%	7.7%
Legal	5.6%	6.4%	3.7%
Manufacturing	4.1%	4.1%	4.3%
Not-For-Profit	5.6%	5.5%	4.2%
Other	4.3%	4.9%	4.3%
Retail & Wholesale	4.7%	4.5%	5.2%
Technology	4.1%	4.6%	5.3%
Transportation	4.5%	5.4%	6.7%

AVERAGE IMPROVEMENT RATES ACROSS ALL INDUSTRIES AND ORGANIZATION SIZES

Following a comprehensive program of new-school security awareness training complemented by regular simulated phishing exercises over the course of a year or more, organizations from various industries and of different sizes have seen significant enhancements in their security postures. **Small** organizations (1-249 employees) experienced an impressive **85% average improvement rate** in security practices, with over half of the industries surveyed reaching or surpassing this average. Notably, the Banking industry achieved the highest improvement rate, reaching 91% versus 88% in the prior year.

Mid-sized organizations (250-999 employees), witnessed a substantial surge—an average security improvement of **85%**. In this size category, 13 industries reported rates of 85% or higher. Impressively, all industries except for Legal exceeded 80% improvement. The Banking industry achieved a noteworthy 90% improvement, which marks a 4-percent-point gain from the previous year.

Among **Large** organizations (1000+ employees), there was a notable average improvement **rating of 87%**, representing a significant increase from the previous year. Standout performances were observed in specific industries, with Consulting reaching 91%, up substantially from 79% prior year. Moreover, the Energy and Utilities industry demonstrated exceptional progress, achieving a 92% average improvement, which showed a slight yet positive increase from an already high 91% prior rating.

The collective data from organizations of varying sizes and industries points to an average improvement rate of 86% from initial testing through more than a year of continued training and testing. This impressive figure serves as compelling evidence to support the adoption of a new-school security awareness training program, demonstrating its efficacy and underscoring the value of such an investment in solidifying an organization's defense against cyber threats.

KnowBe4 finds that the industry-wide **34.3% of untrained users will fail** a phishing test.

Organizations that commit to ongoing training are rewarded with swift improvement. Once trained, only 18.9% of users failed within 90 days of completing their first KnowBe4 training. After at least a year on the KnowBe4 platform, only 4.6% of users failed a phishing test.

Average Improvement
86%

Average Improvement Rates Across All Industries and Organization Sizes

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	91%	90%	88%
Business Services	80%	85%	84%
Construction	86%	86%	86%
Consulting	86%	87%	91%
Consumer Services	83%	84%	85%
Education	88%	83%	85%
Energy & Utilities	87%	87%	92%
Financial Services	88%	85%	89%
Government	84%	85%	84%
Healthcare & Pharmaceuticals	84%	89%	89%
Hospitality	87%	89%	89%
Insurance	87%	85%	84%
Legal	79%	78%	89%
Manufacturing	85%	87%	88%
Not-For-Profit	82%	84%	89%
Other	84%	83%	86%
Retail & Wholesale	85%	86%	88%
Technology	84%	85%	84%
Transportation	83%	81%	81%

2024 INTERNATIONAL PHISHING BENCHMARKS

At the international level, we use a slightly different data set. It does not include separate industries to determine phishing benchmarks regionally across small, medium and large organizations. We included organizations where a definitive country was associated with the customer account so it could be included in the international benchmark analysis. The same benchmarking phases used to measure Phish-prone Percentages across industries were used for the international data set.

	Phase One Initial Baseline Phishing Security Test Results			**Phase Two** Phishing Security Test Results Within 90 Days of Training			**Phase Three** Phishing Security Test Results After One Year-Plus of Ongoing Training		
	BASELINE			90 DAYS			1 YEAR		
Organization Size	**1-249**	**250-999**	**1000+**	**1-249**	**250-999**	**1000+**	**1-249**	**250-999**	**1000+**
North America	29%	32.6%	39.1%	19.8%	19.9%	17.9%	4.3%	4.6%	4.6%
	TOTAL: 35.1%			**TOTAL: 18.9%**			**TOTAL: 4.5%**		
Africa	29.7%	32.8%	38%	23.7%	28.7%	20.2%	3.6%	5.4%	6.2%
	TOTAL: 36.7%			**TOTAL: 22%**			**TOTAL: 5.9%**		
Asia	31.5%	31.6%	27.4%	20.3%	17.6%	16.6%	5.4%	4.5%	5.9%
	TOTAL: 28.4%			**TOTAL: 17%**			**TOTAL: 5.5%**		
Australia & New Zealand	27.8%	32.5%	40.3%	21.4%	20.3%	16.5%	4.9%	5.3%	4.7%
	TOTAL: 34.4%			**TOTAL: 19.1%**			**TOTAL: 5%**		
Europe	26.5%	26.9%	35.6%	19.3%	20.2%	20.6%	4.1%	4.9%	5.9%
	TOTAL: 32.6%			**TOTAL: 20.3%**			**TOTAL: 5.5%**		
South America	32.7%	29.4%	44.9%	24.4%	22.5%	16.8%	5.2%	5.2%	3%
	TOTAL: 39.2%			**TOTAL: 18.7%**			**TOTAL: 3.9%**		
United Kingdom & Ireland	26.5%	30.2%	35.2%	20%	21%	16.5%	4.1%	4.3%	4.8%
	TOTAL: 32.3%			**TOTAL: 18.4%**			**TOTAL: 4.5%**		

REGION

NORTH AMERICA

By Erich Kron

Typical Organization Profile

According to the U.S. Small Business Administration (SBA), as of 2023 there were **33.3 million small businesses in the U.S. More than 99% have fewer than 250 employees, yet they account for almost 47% of total workers nationwide**. While the SBA definition is defined by annual revenue as well as employee count, it is apparent that smaller organizations dominate enterprises in the U.S. when it comes to sheer numbers. This is reflected in the number of organizations included in the report that fall into the category of 249 employees or below, compared to those above 250 employees.

According to IBISWorld.com, public schools and hospitals top the list for biggest industries by employment in the U.S. Organizations in the Education industry showed a somewhat typical average initial click rate of over 31%. Healthcare and Pharmaceuticals had the dubious honor of topping the list with a whopping 45.4% initial click rate.

The good news is that the overall PPP for North America improved dramatically, dropping from roughly 35% to under 19% in just 90 days. By the end of the year, it was down to just 4.5%.

Most Prevalent Issues and Economic Impact

Within the North American region, the U.S. dominated the cyber crime landscape by a significant margin. According to the **FBI's IC3 report from 2023**, the U.S. had 521,652 complaints filed versus 6,601 in Canada and 1,158 in Mexico. Clearly the U.S. is a huge target; however, others in North America should not let their guard down.

Indeed, in November 2023, **five Ontario hospitals reported** that data stolen in a cyber attack had been posted online following a ransomware attack where the hospitals refused to pay the cybercriminals. This resulted in a **proposed $480 million class action lawsuit** against the hospitals.

But hospitals weren't alone. **Even innocent bookstores** paid the price when Indigo Books & Music fell victim to LockBit ransomware, leaving them unable to process payments in the stores for three days and with a website down for about a month. This cost them millions of dollars in sales.

Incidents in Mexico included a significant ransomware attack on the Querétaro Intercontinental Airport, which services over a million people annually. Once again, this was the LockBit ransomware, which steals data and locks down systems. Fortunately, the malware, which was downloaded in a file by an employee, did not impact the security of travelers.

While cyber attacks can be hard on large enterprises, small organizations often have less capital available to deal with the issue. As recent MGM Resorts and Clorox attacks showed, ransomware can be disruptive and severely impact the bottom line. Yet smaller organizations often can't pay employees when no work is being done and no revenue is being generated. The human cost can be high since over **70% of Americans live paycheck** to paycheck and the average ransomware attack lasts about 21 days. It's a recipe for disaster not only for organizations, but for their employees, as well.

Timely reporting of data breaches is still an issue in North America as individual states often define their own reporting timeframes and triggers. For example, in California, **Civil Code §§ 1798.81.5, 1798.82** states a deadline for notification as the "most expedient time possible without unreasonable delay," while **Arizona's Revised Statute §§ 18-551–552** says reporting must happen "within 45 days after determination that a breach has occurred." The lack of a cohesive federal policy is still a challenge.

However, the U.S. Securities and Exchange Commission (SEC) is helping to standardize reporting for publicly traded companies by releasing the following requirement: **"An Item 1.05 Form 8-K will generally be due four business days after a registrant determines that a cybersecurity incident is material."** In other words, progress is being made, but there is still a lot of work ahead.

Cultural Adoption/General Attitude

As the huge target in North America, U.S.-based organizations are aware of the importance of cybersecurity. Even so, many still struggle to secure a budget for their programs. The average security budget for **organizations is 9.9% of the overall IT budget**. Yet industries, such as Education, Retail and Manufacturing—which all have suffered greatly from ransomware and other cyber crime—invest an average of only about 6% of their IT budget in security.

The fight for budget is causing security professionals to look for the most cost-effective methods of securing systems. Security leaders in North America are well aware of the threats and are doing their best to remain secure.

AI Influences

In North America, as with most regions, the impact of AI is a hot topic among security practitioners and executives alike. Threats from AI include enabling greater scalability of attacks by reducing effort and automating tasks, fueling new risks from less skillful cybercriminals. AI-generated phishing messages—including automated translation into many languages—will increase the quality and sophistication of social engineering attacks.

Deepfakes and other deception-focused media generated by AI are also a concern in this region, especially in an upcoming election year.

Nation-state actors have already waged misinformation campaigns, especially through social media, and are expected to use generative AI to further enhance future campaigns.

Key Takeaways

✓ **In this region, the U.S. remains the biggest target**, but Canada and Mexico are not immune and must keep their guard up.

✓ **Small and medium-sized organizations make up a great deal of U.S. commerce and must take measures to ensure business security and continuity.** Smaller organizations must be especially diligent, stewarding their security budget wisely so they can address the biggest threats with the least effort and fewest resources.

✓ Finally, across industries and organization sizes, the application of employee education and **the adoption of a high-quality security awareness program can make a significant impact on the risk of employees clicking on phishing links** or launching malware through social engineering attacks.

N. AMERICA	BASELINE	90 DAYS	1 YEAR
1-249	29%	19.8%	4.3%
250-999	32.6%	19.9%	4.6%
1000+	39.1%	17.9%	4.6%
Average PPP Across All Organization Sizes	35.1%	18.9%	4.5%

AFRICA

By Anna Collard

Typical Organization Profile

Africa is a region of considerable genetic, linguistic, cultural and economic diversity. When examining the state of cybersecurity on the continent, this diversity must be taken into account and, to some extent, explains the wide variety in the security maturity across different countries and sectors.

This year's findings for Africa show that the baseline PPP across all organizations has increased to 36.7% from last year's 32.8%. This means that before receiving any training, more than one in three employees is likely to click on a suspicious link or email or comply with a fraudulent request. Overall PPP varied greatly across African sectors and countries. For example, there has been quite a significant increase in baseline PPP among the large organizations at 38% versus last year's 33%. This could be attributed to the fact that KnowBe4 has expanded its reach into countries and industries across the continent that previously had not been exposed to a lot of cybersecurity awareness.

Most Prevalent Issues

A region of growth, Africa is rapidly increasing its usage of technology and connectivity. But with growth and digitization come new risks and vulnerabilities that can undermine progress. As a result, Africa has had the **most exponential growth in cyber crimes** over the last few years, particularly among small and medium-sized businesses.

African organizations face several key challenges, including the lack of priority by governments, a relatively low level of general cyber awareness and a lack of IT and cybersecurity skills. For Sub-Saharan Africa's economy, 2023 has been a difficult year, with growth slowing to **3.3% from 4% in 2022**. The region is navigating some of the most daunting challenges in the world, including limited resources, urgent humanitarian and development needs, energy crises, poverty and high youth unemployment rates. These challenges may explain a

lesser focus on perceived non-business critical tasks such as cybersecurity culture.

To address rising cyber crime, some African countries have imposed strict regulatory compliance laws. However, most have not. Currently, only 15 of 55 African countries have ratified the African Union Malabo Convention, a legislative framework to foster data protection and general safeguards against cyber crime. Eleven countries have partial laws, and 30 have no meaningful cyber crime laws at all. Governments frequently do not adequately monitor threats, collect digital forensic evidence or prosecute computer-based crime.

The skills shortage persists as one of Africa's biggest cybersecurity issues. The continent faces a growing lack of certified cybersecurity professionals. Many businesses, agencies and consumers lack cyber awareness, and businesses fail to implement basic cybersecurity controls.

Economic Impact

It is difficult to estimate how much cyber crime really impacts the African economy as incidents and financial impact are not officially disclosed. In fact, most cybersecurity incidents go unreported.

The **South African Council for Scientific and Industrial Research (CSIR)** expects an increase in cyber attacks on government departments and critical infrastructure, affecting not just private sector organizations but entire societies and economies. KnowBe4 has conducted multiple **surveys** over the last three years about Africa's preparedness to deal with emerging threats and existing cyber attacks, particularly around cyber extortion and ransomware. The public sector, as well as construction and education sectors, have consistently scored very

low in both general cybersecurity culture and cyber resilience when compared to the financial and banking sectors. This is concerning, as threats to South Africa's critical infrastructure can have a detrimental impact across the region's economy and society at large. Just prior to the release of this report, South Africa experienced multiple serious cyber attacks against their public sector organizations, such as the Companies and Intellectual Property Commission (CIPC) and South Africa's Government Pensions Administration Agency (GPAA).

As experienced during the 2021 ransomware attack against South Africa's Transnet, a state-owned ports authority enterprise, attacks against critical infrastructure can result in devastating economic consequences that go beyond the direct losses experienced by the impacted organization.

Cultural Adoption and General Attitudes

Many African countries face unique and complex socioeconomic landscapes. Some challenges faced internationally are further compounded at the local level. For example, as one of the most unequal countries in the world, South Africa has a high rate of poverty and unemployment rate, factors that contribute to higher crime.

Yet with a median age of just 19.7 years, Africa has the youngest population in the world, and the youth are demanding access to global connectivity and emerging technologies, such as AI. According to KnowBe4's Africa End User Cyber Awareness survey 2023, 63% of respondents use their mobile phone for mobile banking and payments. Sixty-eight percent were concerned about cyber crime, but many lacked some very basic understanding of what type of threats they are exposed to.

AI Influences

Based on KnowBe4's 2023 Generative AI in the Middle East and Africa survey, the sentiment toward AI and new technologies is highly positive, with 26% of respondents using it daily and 42% several times a week. Users of generative AI in Africa and the Middle East reported several benefits, including time saved (80%) and assistance with complex tasks (70%). Moreover, generative AI helps them improve productivity (63%) and enhance creativity (59%). Nevertheless, African users are concerned about the ethical implications, and 90% believe AI tools should be regulated to ensure responsible use.

In another KnowBe4 2023 genAI survey across South African security leaders, over a third (36%) of respondents said their organizations don't address or regulate the potential misuse of generative AI within their organization. Fifty-eight percent of respondents said no specific training is provided about identifying and countering AI-generated misinformation or deepfakes.

...Africa has had the most exponential growth in cyber crimes over the last few years, particularly among small and medium-sized businesses.

Key Takeaways

✓ **Africa is a highly attractive target because of vulnerabilities within many of the region's public sector organizations; a lack of budget, adequate resources and skills shortage;** and the cascading social and economic disruptions that can be achieved by cybercriminals. Many businesses in this region cannot afford even the most basic security controls. Those that can invest struggle to find needed cybersecurity skills.

✓ **Most organizations in Africa are embracing emerging technologies and embedding them into day-to-day operations.** However, not enough is being done to regulate their use or educate users on risks, including disinformation, security and privacy, ethical concerns (such as bias), inaccuracies and impact on critical thinking.

✓ **These are challenges that need to be addressed through a combination of regulation, guidelines and awareness training.** Special attention should be given to threats posed to society through malicious use of new technologies, such as deepfakes, especially when used for political manipulation. Major elections coming up in South Africa and other areas of the continent will drive the need for education campaigns. More public-private partnerships are required to assist Africa's public sector and small to medium-sized organizations to build capacity, address the skill shortage and become more resilient in the ever-growing digital world. Collaboratively investing in Africa's youth and providing cybersecurity training opportunities and exposure will not only fill the urgent skills gap but also address the youth unemployment problem.

AFRICA	BASELINE	90 DAYS	1 YEAR
1-249	29.7%	23.7%	3.6%
250-999	32.8%	28.7%	5.4%
1000+	38%	20.2%	6.2%
Average PPP Across All Organization Sizes	36.7%	22%	5.9%

ASIA

By Philip Tnee and Jeremy Schwartz

Most Prevalent Issues

Bad actors in the Asia-Pacific (APAC) region have upped their game in recent years. Cyber attacks targeting sensitive data in both private and public entities have increased in frequency, complexity and incisiveness.

The Allianz Commercial Risk Barometer for 2024 identifies cyber risk as the primary concern for businesses in APAC, with malware, ransomware and social engineering attacks being the most common attack strategies. Criminals often use emails, websites and social media for these deceptive attacks.

Governments across APAC are spearheading strategies, enforcing laws, building defensive capacities and championing international cooperation to fortify regional defenses against cyber attacks. The Association of Southeast Asian Nations (ASEAN) released its 2021-2025 ASEAN Cybersecurity Cooperation Strategy, which provides a "roadmap for regional cooperation to achieve the objective of a safe and security ASEAN cyberspace." ASEAN includes the member states of Brunei Darussalam, Cambodia, Indonesia, Myanmar, Lao PDR, Malaysia, Philippines, Singapore, Thailand and Vietnam.

Singapore's Cybersecurity Act has been in force since 2018, and on December 15, 2023, the Cyber Security Agency of Singapore (CSA) published a consultation paper on a draft Cybersecurity (Amendment) Bill 2023 (Bill).

Economic Impact

At of the end of 2023, the APAC region accounted for nearly a quarter (23%) of global cybersecurity incidents, according to the IBM X-Force Threat Intelligence Index. The impact of these attacks extends far beyond mere financial losses, inflicting significant damage to organizational reputations, operations and customer trust. The ripple effects are felt across entire industries, hampering growth and innovation.

Financially, the costs associated with cyber crime in the APAC region are projected to skyrocket into the trillions by 2027. High-profile incidents, such as the SingHealth breach and the Bangladesh Bank heist, have served as stark reminders of the far-reaching consequences of cyber vulnerabilities. In the SingHealth breach alone, the personal data of 1.5 million Singaporeans was compromised, highlighting the grave implications for individual privacy.

Typical Organizational Profile

Healthcare, technology, manufacturing and tourism stand as dominant economic drivers in the APAC region. The security needs of organizations operating in these sectors can vary considerably, increasing the complexity of needed cybersecurity defense strategies.

The digital landscape in the region is experiencing a boom, introducing new vulnerabilities amid this growth. The APAC economy is expected to experience a regional growth rate of around 4.2% in 2024, although this growth is not without its challenges.

Benchmark Data

To accurately assess the region, KnowBe4 analyzed the results of approximately 600,000 phishing simulation tests delivered to just over 1,200 organizations in APAC. Of these, 59% of the organizations are small (1-249 employees), 26% are medium (250-999 employees) and 14% are large (1000+ employees).

In APAC, the initial baseline phishing security test results averaged 28.4%. That means that before receiving any training, almost one out of three employees is likely to click on a suspicious link or email or comply with a fraudulent request. However, this figure puts the region well below the global baseline average of 34.3%, suggesting increasing focus on cybersecurity concerns is paying dividends. Large organizations had the lowest baseline average at 27.4%, with medium and small organizations effectively tied around 31%.

Cultural Adoption and General Attitudes

High-profile breaches and the driving force of government regulations seem to be raising the region's cybersecurity consciousness. While employees are gradually recognizing their personal responsibility in maintaining cybersecurity, the extent of this recognition varies considerably, heavily dependent on the organization's culture and the intensity of its training initiatives.

Cultural factors, such as the emphasis on hierarchy and deference to authority in certain APAC societies, can also influence the adoption of cybersecurity best practices. Linguistic and cultural diversity further complicate the challenge of establishing a unified security culture across the continent, underscoring the importance of tailored and inclusive approaches to cybersecurity education and awareness.

Cybersecurity training is steadily gaining prominence, propelled by policy mandates and the pressing need to stay ahead of increasingly sophisticated threats. However, the adoption of training practices remains a varied landscape across the vast and diverse APAC theater.

Organizations in the region comprise tech and security professionals, regular employees who are well-versed in identifying phishing attempts and compliance teams, all playing crucial roles in cyber defense. Their arsenal includes engaging security awareness training, phishing simulations, endpoint protection, firewalls, cloud security measures, access controls and robust data encryption protocols. However, adoption and effectiveness of these measures can vary significantly between organizations.

AI Influences

Like all technologies, AI presents both great opportunities and threats regarding cybersecurity. AI isn't new. What is novel is the rapid advancement of deepfake technologies and large language learning models, such as OpenAI's GPT (which powers ChatGPT), with the addition of voice, image and video generation. These new advancements introduce additional potential red flags. Cybercriminals are still focusing on attaining the human emotional response with social engineering.

At of the end of 2023, **the APAC region accounted for nearly a quarter (23%) of global cybersecurity incidents,** according to the IBM X-Force Threat Intelligence Index.

Organizations and individuals are concerned with AI and how it has added a new strain of cyber crime with potentially devastating effects. Calls continue for more regulation and legislation to protect the region from AI. Released in January 2024, The Engaging with Artificial Intelligence (AI) report is a collaboration among 13 international organizations, including the Cyber Security Agency of Singapore (CSA) and other Asia-based organizations.

On the flipside, AI is emerging as a potent new arsenal in the cyber defense toolkit, capable of predicting, detecting, analyzing and responding to threats on an unprecedented scale. The APAC region is proactively pooling resources and expertise to foster the positive potential of AI while hedging against its negative implications. Initiatives like the ASEAN-Singapore Cybersecurity Centre of Excellence are focused on developing AI-based cybersecurity solutions and fostering regional collaboration in this domain.

Key Takeaways

✓ **APAC is surfing a rising wave of cyber threats**, spotlighting the need for state-of-the-art defenses.

✓ **AI is revolutionizing defensive strategies against cyber attacks, enhancing detection, prediction and response.** AI also presents new challenges as adversaries leverage AI for offensive purposes.

✓ **The human layer of security is pivotal.** Cultivating an engaged, well-informed workforce that transcends language and cultural hurdles is as vital as any high-tech solution.

ASIA	BASELINE	90 DAYS	1 YEAR
1-249	31.5%	20.3%	5.4%
250-999	31.6%	17.6%	4.5%
1000+	27.4%	16.6%	5.9%
Average PPP Across All Organization Sizes	28.4%	17%	5.5%

AUSTRALIA AND NEW ZEALAND

By Joanna Huisman and Joe Gillett

Most Prevalent Issues

Compared to other evaluated regions in 2024, the results for Australia and New Zealand (ANZ) are comfortably in the mid-range across organizational size categories. The most notable improvement in ANZ was observed within Large organizations, where the initial PPP at Phase 1 of 40.3% was substantially reduced to 4.7% in Phase 3, an 88.28% improvement. This significant favorable movement serves as a testament to the efficacy of robust and continuous security awareness training, along with rigorous testing protocol, in strengthening cyber defenses.

Medium organizations also realized a considerable enhancement, with an 82.7% improvement from Phase 1 to Phase 3, while Small organizations followed closely with an advancement of 81.6% over the same phases. These improvements further underscore the benefits of sustained security awareness initiatives across different organizational scales.

Typical Organization Profile

As of June 2023, Australia plays host to 2,589,873 active businesses within its economy. The business landscape in Australia is predominantly composed of small businesses. Across Australia, a staggering 97.3% are characterized as small (0-19 employees), while mid-sized organizations (20-199 employees) make up 2.5%. Large organizations (200+ employees) account for a mere 0.2% of the total business count, as categorized by the Australian Bureau of Statistics.

Additionally, during the fiscal year 2022-2023, the industries experiencing the most significant growth in organizational counts included Healthcare & Social Assistance, Financial & Insurance Services and Transport, Postal and Warehousing. Conversely, the Administrative and Support Services along with the Retail & Trade industries witnessed the most notable declines in business numbers.

New Zealand's business landscape continues to expand, with 1.8% growth from the previous year, bringing the total number of organizations to 605,000. According to classifications provided by Infometrics, a vast majority (96.3%) fall into the small business category (0-19 employees). Medium-sized businesses (20-199 employees) constitute 3.1% of the total count. Meanwhile, large organizations (200+ employees) are relatively rare, representing just 0.5% of New Zealand's organizations.

According to Statista, for the fiscal year concluding June 2023, New Zealand's primary industry export revenues were led by the Dairy industry. Following Dairy, the Meat & Wool industries also made a substantial contribution. However, the Healthcare and Social Assistance industry continues to be the largest employer.

Oceania encompasses a sprawling group of thousands of islands scattered across the Central and Pacific Ocean. This expansive region includes Australia and New Zealand. Dominated by the Pacific Ocean, Oceania's name reflects the pre-eminence of the Pacific in shaping its identity and economy. For the scope of this study, Australia and New Zealand are addressed separately due to their notable size and economic stature relative to the smaller island nations composing the remainder of the region. Oceania's varied economies leverage key industries such as Lumber, Commercial Fishing and Mining, yet it is the tourism industry that significantly propels economic activity across these Pacific communities. Despite the challenge in obtaining comprehensive data on organizational scales in this context, available indicators suggest that the region is predominantly home to small-scale entities, with some mid-sized organizations interspersed throughout.

Most Prevalent Issues

The Australian Signals Directorate (ASD) Cyber Threat Report disclosed that their response efforts encompassed 1,100 cybersecurity incidents involving Australian entities. In a distinct tally, close to
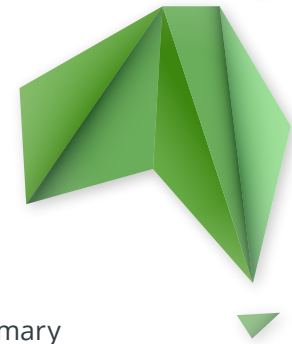
94,000 cyber-related reports were submitted to law enforcement via ReportCyber. That comes out to approximately one report every six minutes—a staggering 24% increase over the prior year. KPMG research shows that over 693,000 businesses experienced a cyber attack, a 33% bump over the prior year, and the cost of cyber crime in Australia totaled $29 billion. Additionally, KPMG shared that approximately 60% of all attacks hit small and mid-sized businesses. The primary methods employed by cybercriminals to infiltrate organizations include email compromise, business email compromise and online banking fraud. Under the Notifiable Data Breaches (NDB) scheme, any organization or agency the Privacy Act 1988 covers must notify affected individuals and the Office of the Australian Information Commissioner (OAIC) when a data breach is likely to result in serious harm to an individual whose personal information is involved.

According to the OAIC, from July to December 2023, Health Service Providers, Finance, Insurance, Retail and Government were the top-five industries hit with data breaches. The principal origins of these attacks can be attributed to system vulnerabilities (up 21%), deliberate malicious activity (up 12%) and human error (up 36%). Malicious attacks and phishing remain the leading cause.

Based on data from cybersecurity watchdog CERT NZ, the landscape of reported cybersecurity incidents and their financial repercussions of New Zealand in 2023 showed modest improvement. There were 7,935 incidents reported in 2023. Approximately 2,000 of those occurred in Q1 with a financial impact of $5.8 million. That reflects a slight decrease of 3% compared to figures from 2022. Submissions of incident reports came from diverse sources across all industries and organization sizes. Among incidents registered with CERT NZ, 24% involved financial loss. The cumulative financial detriment reported amounted to $18.3 million, underscoring the significant economic impact of cyber incidents on affected entities.

Economic Impact

As reported by Australian risk management firm Gallagher, cybercriminals are continuously enhancing and sophisticating their strategies to conceal their activities and maximize their illicit gains from victims through a variety of criminal endeavors. For victimized businesses, the financial toll is steadily climbing year over year. Gallagher estimates the impacts of cyber incidents average up to $45,000 for small businesses, up to $97,000 for mid-sized businesses and up to $72,000 for large businesses.

Cybersecurity breaches can have a profound impact on businesses globally, often remaining undetected for extended periods. The identification and resolution of such attacks may take several months, during which time organizations may suffer operational disruptions that can severely undermine their financial stability. The risks are particularly acute in regions such as Oceania, where preparedness levels among individuals and enterprises may be lower, exacerbating vulnerability to cyber threats.

Furthermore, the shortage of trained cybersecurity professionals is a critical issue worldwide. This talent gap places additional pressure on existing employees, who may be compelled to address complex cybersecurity challenges without adequate expertise. Such circumstances not only strain the workforce but also increase the risk of inadequate threat mitigation, potentially compounding the consequences of cyber incidents.

Cultural Adoption/General Attitude

Interest in security culture within the region has progressively gained momentum, expanding into untraditional areas. There is a growing recognition by IT of the imperative for integrating change management with cybersecurity strategies to deeply resonate with and mobilize employees. Over the preceding year, executive awareness and comprehension of cybersecurity have surged, with its acceptance as an enterprise-wide risk now prevailing at the board level. These positive trends underscore significant progress in the advancement of a robust cybersecurity culture across Australia and New Zealand.

The Oceania Cyber Security Center's analysis reveals that while the region has historically exhibited more advanced technological capabilities, human factors lagged in prior years. Despite notable improvements following targeted initiatives, current security culture ratings highlight the opportunity to enhance and align human capabilities with the region's technological strengths.

This situation underscores the essential need to cultivate a security-conscious culture within organizations. It's imperative that employees are not only educated about their vital role in safeguarding the company's digital assets but also demonstrate a consistent adherence to cybersecurity best practices in their daily activities. By fostering an environment where security protocols are understood and actively practiced, businesses can reinforce their defenses and enhance their resilience against the evolving threat landscape.

Following recent developments in government regulations, there has been a notable shift toward the adoption of more secure practices among organizations. While there is a broad consensus that fostering a security-conscious culture is imperative, organizations often grapple with the challenge of cultural transformation. Despite the overarching agreement on its importance, there's a tendency to continue relegating the responsibility for this cultural shift to IT departments, indicating an area that requires further strategic attention and cross-functional collaboration.

AI Influences

Entities and individuals throughout the region are expressing concern over the emergence of AI as a conduit for cyber crime that could lead to catastrophic consequences. While it's universally acknowledged that AI can exert a beneficial influence across various facets of society, its swift introduction has precipitated the advent of deepfakes in imagery, audio and video, further complicating the detection of traditional social engineering threats. Such technological advances require a reckoning with the heightened emotional responses they can provoke in humans.

Consequently, there is an overarching demand for enhanced regulatory measures and legal frameworks to safeguard the region against the perils and exploitation associated with AI. In response to these issues, the Australian Government issued a provisional statement on January 17, 2024, committing to the promotion of responsible AI usage. Furthermore, the Engaging with Artificial Intelligence (AI) report, unveiled in the same month, represents a joint effort among 13 global agencies, including prominent institutions such as New Zealand's

CERT NZ, the National Cyber Security Centre, the Australian Signals Directorate, and the Australian Cyber Security Center, to address these burgeoning challenges.

3 Key Takeaways

✓ **As the threat landscape continues to evolve, cyber crime is expected to intensify.** Consequently, it's crucial for this region to place strong emphasis on bolstering security awareness through comprehensive and rigorous testing programs designed to enhance workforce cyber resilience.

✓ **The region currently exhibits a lack of preparedness for the burgeoning impact of AI.** To bridge this gap, it is imperative to embrace a proactive strategy focused on education and significant investment in AI-related initiatives, ensuring that the local ecosystem is well equipped to navigate and capitalize on the AI revolution.

✓ **This region stands to benefit from greater cooperation in exchanging intelligence on cyber threats.** Participation in a global information-sharing network is critically important as it provides more profound insights into emerging dangers and facilitates access to cutting-edge concepts and techniques in the field of cybersecurity.

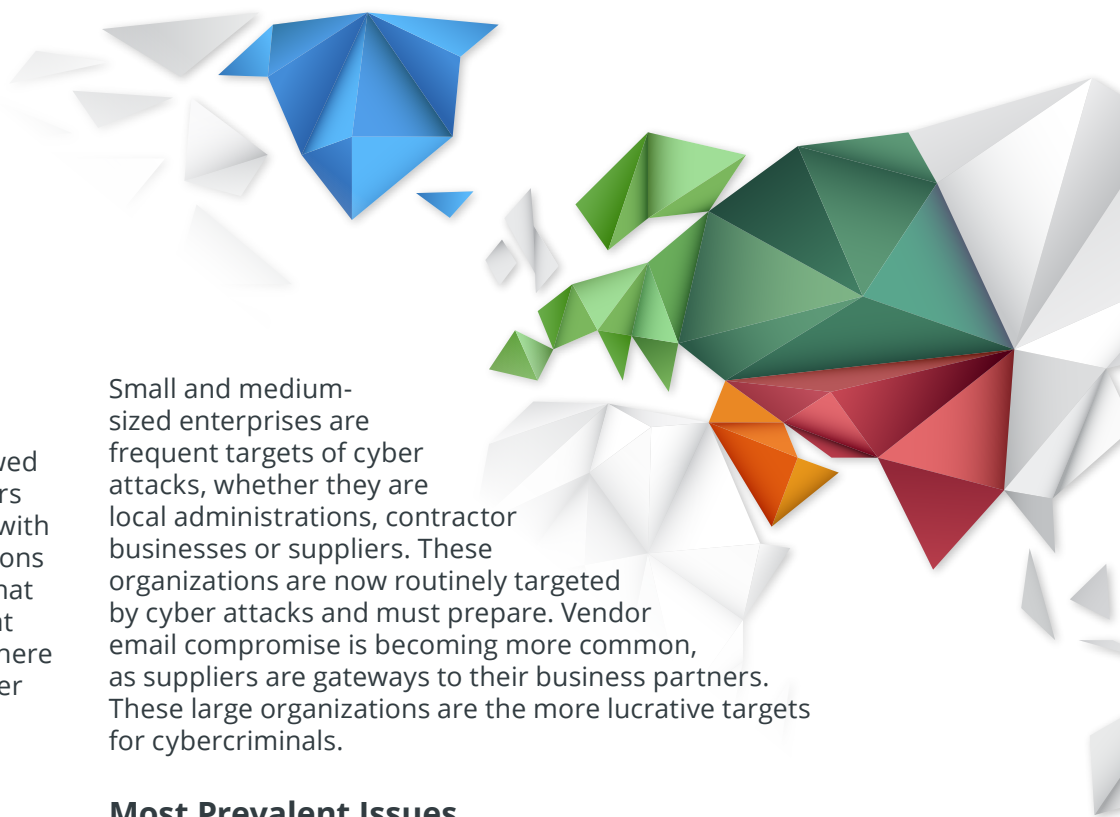| AUSTRALIA & NEW ZEALAND	BASELINE	90 DAYS	1 YEAR
1-249	27.8%	21.4%	4.9%
250-999	32.5%	20.3%	5.3%
1000+	40.3%	16.5%	4.7%
Average PPP Across All Organization Sizes	34.4%	19.1%	5%

EUROPE

By Martin Kraemer

Benchmark Data

Compared to those featured in the 2023 report, the organizations included in 2024 demonstrated a decline in performance. Across all organizational sizes, baseline performance was down by 3.2%, 90-day performance was up by 0.6%, and one-year performance was down by 1.5%. European organizations across the three different sizes (1-249, 250-999 and 1000+ employees) performed better than the worldwide average. Small organizations (26.5%) performed best before training, followed by medium (26.8%) and large (35.6%) organizations. These numbers are almost unchanged from last year and more or less consistent with earlier years. These stagnant results suggest that many organizations have yet to step up their security awareness efforts, recognizing that the human element is a crucial part of their cyber defense and that phishing is the number-one attack vector for social engineering. There is some hope as European organizations perform on average better before training than the rest of the world.

Typical Organization Profile

Europe has a growing number of small and medium-sized enterprises. The vast majority of enterprises have 10-49 employees and less than one percent of all organizations have more than 250 employees. More than 70% of small organizations have a low or very low digital intensity according to a Eurostat report. Medium organizations further in their digital transformation journey (only about 40% with low or very low ratings) and less than 20% of large organizations fall into that category. The indicator is based on a range of metrics, such as the use of remote working tools and online conferencing software, the presence of security measures and the use of robots in manufacturing.

Small and medium-sized enterprises are frequent targets of cyber attacks, whether they are local administrations, contractor businesses or suppliers. These organizations are now routinely targeted by cyber attacks and must prepare. Vendor email compromise is becoming more common, as suppliers are gateways to their business partners. These large organizations are the more lucrative targets for cybercriminals.

Most Prevalent Issues

According to the ENISA Threat Landscape 2023 report, organizations in the region are frequently targets of DDoS and ransomware attacks. While social engineering attacks with AI and other new techniques are on the rise, phishing remains the number-one attack vector. The region also was subjected to the worldwide trend of new extortion tactics as cybercriminals continued to professionalize their as-a-service programs. The most targeted sector was public administration, followed by attacks on individuals and the healthcare sector. The European Network and Information Security Agency (ENISA) also reports an increase in information manipulation as observed in the context of Russia's war in Ukraine and an overall increase in geopolitical motivations of cybercriminals.

Overall, the situation is similar to previous years. Ransomware remains one of the biggest cyber threats with phishing as its most common attack vector. Close attention should also be paid to supply chain attacks, which are rising in prevalence.

Economic Impact

The true impact of cyber crime is hard to determine, but individual cases show that severe consequences of data breaches are possible. The cumulative extent of financial consequences was estimated to be about 0.84% of Europe's annual GDP according to a 2018 report from Upguard. Since then, we have seen high-double-digit growth of ransomware year over year, again and again. It is unlikely that cyber crime will slow any time soon. In fact, cyber crime is now considered to be the world's third-largest economy.

The economic impact in Europe can also be judged based on the severity of recent data breaches—from medical insurance companies in France being targeted and leaking data of 33 million citizens to the aftermath of the MOVEit vulnerability that impacted more than 100 organizations across Europe. Among them are many public administrations in Germany. In the UK, credit scoring agencies advised customers to freeze their scores. Ransomware gangs continued to hit Europe hard and employed new extortion schemes. The joint effort of law enforcement, coordinated by Europol, to take down the LockBit ransomware gang has led to more breaches becoming public as a result of the investigation. While the long-term effect of the takedown remains uncertain—involved cybercriminals are likely to regroup—losing access to infrastructure is a considerable setback.

Europe is also subject to some of the more stringent regulatory regimes worldwide led by the European Union. Legislation such as the General Data Protection Regulation (GDPR), the Network and Information Systems Directive (NIS2) and the Digital Operational Resilience Act (DORA), among others, require organizations to dedicate resources. Compliance with legislative requirements is mandatory and failure to comply results in severe fines that can substantially affect businesses' bottom lines.

Cultural Adoption/General Attitudes

Across Europe, attitudes about cybersecurity differ widely. This includes how people understand its importance, how they perceive responsibility in corporate contexts and the degree to which they feel empowered to protect themselves. Generally speaking, central mainland Europe, including the United Kingdom and Ireland, are more cyber-aware and host more mature businesses when it comes to cybersecurity. This is consistent with findings from KnowBe4's Security Culture Report, which reveals that the understanding and prioritization of cybersecurity within corporate environments are less advanced in Western, Eastern and Southern Europe compared to other regions.

When it comes to security awareness, there is a growing understanding that the entire workforce must be part of an organization's cyber defense. The importance of empowering people to protect businesses is recognized across organizations of all sizes and sectors. However, the extent to which that recognition drives strategic change to make cybersecurity a business priority varies largely. While views on cybersecurity may have shifted from "checkbox exercise" to "strategic initiative," implementation of the required change is progressing slowly.

Only 32% to 35% of European organizations assess their cyber risks more than once a year, according to the ISACA State of Cybersecurity Report 2023. This number has been consistent over the last three years and underscores organizations' challenges in aligning resources with requirements. This includes continued budget restrictions and the cybersecurity skills shortage, which remains one of the major challenges. There are simply not enough people available to make major strides.

AI Influences

ENISA recognizes misinformation and disinformation as a cybersecurity threat to organizations. The prime example is attacks targeting organizations that support Ukraine's defense against Russia. Following disinformation campaigns, cybercriminal groups target those organizations. Misinformation and disinformation are now fueled by AI allowing threat actors to spread falsehoods more quickly and easily.

Organizations in Europe, like elsewhere, are also eager to benefit from an early adoption of generative AI-powered tools. With a traditionally more risk-aware mindset, many corporations have a variety of privacy, security and further ethical risks involved, leading to a relatively more reserved approach. An example of this was Italy's data protection watchdog temporarily banning the use of ChatGPT. Meanwhile, the tool has returned to the country. Organizations will continue to implement required safeguards for AI-powered tools and must continue training their employees.

The worldwide onslaught of phishing emails—powered in part by AI—also affects European organizations. While phishing emails continue to follow familiar patterns, spear-phishing and pretexting attacks show the use of AI. Although these are still the early days of AI-powered phishing, organizations must expect further professionalization and automation of phishing-as-a-service. Phishing will remain the primary attack vector.

Key Takeaways

✓ European organizations perform, on average, better than the rest of the world, indicating an increasing appreciation for cybersecurity and a general awareness of online scams, which we might attribute in part to the much-discussed stringent regulatory and legislative landscape.

✓ Organizations are falling a bit behind when it comes to sustained long-term engagement, with the PPP for medium and large enterprises lagging the worldwide average.

✓ The region needs to continue to evolve with its regulatory regime on data protection and AI to stay at the forefront of cybersecurity as organizations start to adopt AI tools.

EUROPE	BASELINE	90 DAYS	1 YEAR
1-249	26.5%	19.3%	4.1%
250-999	26.9%	20.2%	4.9%
1000+	35.6%	20.6%	5.9%
Average PPP Across All Organization Sizes	32.6%	20.3%	5.5%

SOUTH AMERICA

By Joanna Huisman

Benchmark Data

In 2024, South American organizations across most size categories demonstrated impressive performance improvements, initially recording the highest baseline PPP across all regions for small (32.7%) and large (44.9%) entities. Notably, in the large organizations category, South America achieved the most significant improvement after one year, showcasing a significantly lower PPP of 3%. This 93.2% reduction from the baseline affirms the efficacy of thorough and persistent security awareness training and testing regimes in enhancing cyber resilience.

Substantial positive shifts in metrics from one year to the next suggest a transformative shift within the security culture landscape. Such trends imply that employees are increasingly internalizing a security-conscious mindset, recognizing their role in fortifying the company's defenses and acting in ways that align with this heightened sense of responsibility. This behavioral change is indicative of a maturing organizational attitude toward cybersecurity, with proactive measures and informed vigilance becoming embedded in daily practice.

Typical Organization Profile

Research shows that small and medium-sized organizations make up 99.5% of all businesses in the region, underscoring the high stakes of cyber defenses. According to the United Nations Development Program (UNDP), these small and medium-sized organizations account for roughly 60% of employment and contribute 25% of the region's GDP. These companies' economic significance underscores the crucial necessity of safeguarding their assets against potential cyber attacks.

The implementation of robust security protocols for digital devices and the deployment of comprehensive, consistent and continuous security awareness training across all size organizations is imperative. While enlisting expert providers of content and testing is ideal, there are also readily available free options that can serve as a starting point

to launch essential cybersecurity initiatives. Given the immense scale of cybersecurity threats, education and prevention measures need to be easily accessible to everyone. To strengthen our defenses against cyber attacks, we must ensure that there are no obstacles hindering people from accessing these vital resources. The adoption of internal champion programs—in which designated employees act as cybersecurity advocates—can be highly effective in ensuring that awareness and best practices reach even the most isolated sectors of the organization.

Most Prevalent Issues

South America was one of the two regions globally that experienced increased data breaches. (Antarctica was the other.) Security incidents compromised upwards of two million accounts as detailed by Infosecurity Magazine. A recent report from cybersecurity firm Trend Micro reveals Brazil as the country ranking second globally in susceptibility to cyber attacks. In the list of nations facing the highest number of thwarted cyber threats in the first half of 2023, Brazil is outpaced only by the United States. The report indicates that approximately 85.6 billion cyber threats were intercepted worldwide during the first six months of the year, accounting for 59% of the annual total reported in 2022. Following the United States and Brazil, India occupies the third place in the hierarchy of countries most frequently targeted by hackers.

According to the Council on Foreign Relations, the lack of attention given to South America in the global cyber conversation is the result of at least three factors. First, threat intelligence firms often have limited motivation to concentrate on South America when compared to more sizable markets, adding to the lack of public awareness. That serves to widen the gap and exchange of intel between the public and private sectors. Additionally, there is a prevalent bias within the cybersecurity industry to focus exclusively on well-known threat actors, overlooking those that are on the rise. Lastly, the uneven levels of development throughout the region result in a wide disparity in cybersecurity requirements among the countries. Coordinated defense mechanisms across the region are scarce.
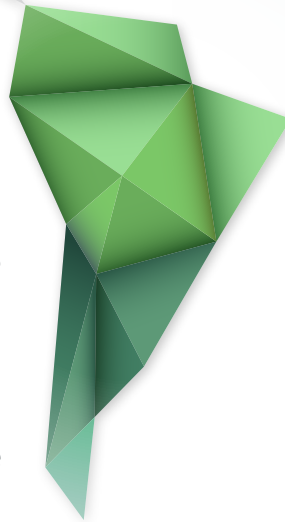
Economic Impact

Experts estimate that the economic impact of cyber attacks on countries in South America is significant, equating to approximately 1% of GDP. This figure could escalate to as much as 6% if critical infrastructure is compromised. According to a study by Fortinet, 31% of organizations in South America reported incurring expenses exceeding $1 million as a result of cyber attacks. Furthermore, these figures are on an upward trajectory, with costs associated with cyber attacks expected to continue rising.

Describing the cybersecurity posture in this region as merely reactive doesn't fully capture the extent of the issue. Because of the reactive approach, research shows there's a danger that governments in South America may develop distorted views of the actual threat landscape. While high-profile ransomware attacks have undoubtedly paralyzed federal and local government operations, a large portion of security breaches and vulnerabilities can be attributed to a fundamental shortfall in implementing basic cybersecurity measures by both public and private organizations.

There is good data and direction because of the Organization of American States (OAS), which stands out as the foremost regional platform addressing cybersecurity issues. Over the past decade, the OAS has spearheaded various initiatives, including conducting cyber simulations, promoting capacity-building efforts and assisting in the formulation of national cybersecurity strategies for its member states. The OAS, coupled with the United Nations Economic Commission for Latin America and the Caribbean (ECLAC), has been actively working to intertwine the development agenda with cybersecurity initiatives. In developing nations, the capacity to recover from devastating cyber attacks is limited. Also, the landscape is further challenged by insufficient investments and low levels of preparedness among citizens and government entities alike. This situation casts a worrying and foreboding shadow over the future of cybersecurity resilience in this region.

Recognizing this as a matter of national interest, the President of Brazil established the National Cybersecurity Committee (CNCiber) on December 27, 2023. This body is tasked with evaluating and proposing measures to enhance cybersecurity in Brazil. Comprising 25 members, it includes representatives from the government, civil society, private sector and technological institutions. This demonstrates significant progress in protecting Brazilian organizations and will undoubtedly lead to an increase in the country's cybersecurity maturity.

Cultural Adoption/General Attitude

Despite historically trailing advanced economies in the realm of digitization, South American countries have recently been making significant strides in embracing and advancing digital services and technologies for their citizens. According to Statista, as of early 2023, an estimated 75% of the region's population had internet access, outpacing the worldwide average of 65%. Notably, Brazil and Argentina boast penetrations above 80%. In addition, citizens are being encouraged to engage in mobile banking and to participate in online shopping. Considering the low level of citizen cyber readiness combined with the accessibility of novel digital practices, there is cause for great concern and caution that cybersecurity is being overlooked in the name of digital advancement.

Experts forecast a robust expansion of e-commerce activity in the region, projecting a 27% surge in transaction volume that was expected to hit $509 billion in 2023. The government's position to heighten inclusion in the global marketplace is stretching citizen capabilities and encouraging cyber attacks to keep growing. According to Reuters, residents of the region demonstrate a high degree of engagement with emerging technologies, positioning them as ideal candidates for all kinds of digital scams. What these organizations are missing is employees with the expertise to proactively identify, report and prevent cyber attacks. They face challenges in integrating security awareness training into their workforce effectively, and the sluggish rate of implementation is hindering its efficiency. The rapidity of their embrace of digital adoption is outpacing the acquisition of necessary knowledge to ensure its secure use.

AI Influences

AI is predicted to significantly enhance South America's economic output, with estimates suggesting a potential increase of more than 5% in the region's GDP by 2030. These forecasts are expected to climb even higher should governments implement strategic policies focused on AI-related talent development and the expansion of digital infrastructure. Cultivating a skilled workforce is crucial for a thriving AI sector in South America, as is the establishment of strong regulations to guarantee ethical AI deployment and advancement. Studies indicate that the region's commitment to digitization will accelerate AI integration in businesses seeking operational efficiency and market agility. Enhanced computing capabilities and greater adaptability to market shifts are expected to further drive the advancement. In the realm of government, AI presents a unique chance for South American authorities to tackle and overcome enduring obstacles, setting the stage for substantial social and economic progress. Still, the AI policy landscape in this region is marked by significant policy volatility, with new administrations often altering or abandoning policy initiatives set by their predecessors.

Key Takeaways

✓ **Varied stages of development across South America have led to a broad range of cybersecurity needs among different countries.** There is a notable lack of coordinated defense mechanisms spanning the region, leading to significant disparities in cybersecurity preparedness and response.

✓ **The pace of digitization is accelerating rapidly.** Given the limited cyber readiness of the population, widespread adoption of new digital practices creates significant cause for concern.

✓ **Organizations are grappling with a shortfall of personnel skilled in the proactive detection, reporting and prevention of cyber attacks.** The challenge lies in embedding effective security awareness training and testing within their workforce.

S. AMERICA	BASELINE	90 DAYS	1 YEAR
1-249	32.7%	24.4%	5.2%
250-999	29.4%	22.5%	5.2%
1000+	44.9%	16.8%	3%
Average PPP Across All Organization Sizes	39.2%	18.7%	3.9%

UNITED KINGDOM & IRELAND (UK&I)

By Javvad Malik

Benchmark Data

Compared to last year, overall PPP across all organizations dropped from 35.2% to 32.3%. While small organizations remained the same, mid-sized organizations performed slightly more poorly compared to last year with a 2% increase in PPP. However, large organizations improved the most, dropping nearly 5% from 39.6% last year to 35.2% this year.

The improvement in large organizations could be attributed to the maturity of hybrid working and mechanisms for promoting a strong security culture.

One of the key takeaways this year is that after a year of frequent and continuous security awareness training and simulated phishing, the average baseline has dropped to 4.3%, a significant improvement from the 5.8% of last year's report. This result underscores the effectiveness of regular and appropriate training regardless of where an organization starts.

Most Prevalent Issues

With the continued conflicts in Ukraine and the Middle East and increasing cyber tensions with China, the UK&I region faces an ever-increasing threat from nation-states and other global actors. The last year has seen an increase in nation-state actors targeting critical national infrastructure (CNI). The National Cyber Security Centre (NCSC) specifically identifies China, Russia, Iran and the Democratic People's Republic of Korea (DPRK) as posing the biggest threats.

Ransomware persists as one of the most prevalent threats facing the UK&I, and phishing remains the most utilized initial access vector. This serves as a reminder that the human factor should not be ignored and that a strong security culture is imperative to protecting organizations.

With a general election upcoming, there is a risk of disruption and disinformation campaigns being used to influence the outcome and/or divide the population. While not purely a cybersecurity issue, it is one that's considerably enabled through cyber.

Finally, we're seeing an increase in attacks not just against organizations, but also high-risk individuals, with an ongoing trend to persistently target those people who may hold sensitive information. Therefore, cybersecurity is not limited to securing corporate accounts, but also personal and social media accounts and devices.

Economic Impact

The economic impact of security breaches has always been tough to determine. Even for a single organization, it can be difficult to quantify all the direct and indirect costs of a security breach.

According to the National Fraud and Cyber Crime Dashboard, over the year, there were just under 400,000 reports with reported losses of £2.3 billion ($2.9 billion), equating to an average loss of £5,750 ($7,154). But it's important to note that the majority of reported cases are from individuals and not organizations. The Cyber Security Breaches Survey from the Department of Culture, Media and Sport puts the average annual cyber crime cost for businesses at approximately £15,300 ($19,000) per victim.

However, the larger the organization, the more severe the consequences. Costs related to the ransomware attack on the British Library were estimated at £7 million ($8.7 million). Royal Mail spent over £12 million ($14.9 million) on recovery costs after its attack, and the attack on Capita cost the British outsourcing company £20 million ($24.9 million).

Cultural Adoption/General Attitudes

General attitudes vary greatly across organizations in the UK&I. Most have an understanding of security awareness. However, an increasing number of organizations, particularly large ones, are moving beyond awareness to focus on behavioral change and security culture.

According to the UK Government, around 71% of organizations report that cybersecurity is a high priority for their senior management. However, in the shadow of a tough economy, many organizations, particularly smaller ones, often sacrifice cybersecurity in favor of keeping the show on the road.

We have seen some organizations shift their approach to building a strong cybersecurity culture by moving the departments responsible for cybersecurity awareness and culture out of the CISO organization, which often prioritizes technical issues. Aligning with more people-centric objectives, some are hiring leaders with marketing backgrounds to better understand how to promote cybersecurity messaging.

While this is still rare, it is a positive sign that organizations are looking to move beyond security awareness as a mere compliance effort and to use it as a tool to make a real difference.

AI Influences

Like most of the world, the UK&I are paying close attention to AI and its impact on cybersecurity.

From a criminal perspective, AI is lowering the barrier of entry to novice criminals, allowing relatively unskilled threat actors to carry out more effective access and information-gathering operations.

The near-term impact of AI on the cyber threat assessment, published by the NCSC, concludes that AI is already being used in malicious cyber activity and will almost certainly increase the volume and impact of cyber attacks—including ransomware—in the near term.

Analysis from the National Crime Agency (NCA) suggests that cybercriminals have already started to develop criminal Generative AI (GenAI) and to offer GenAI-as-a-service. But these are still in the early stages of development.

Bear in mind, though, that from a cybersecurity perspective, AI doesn't represent a revolution. It's more of an evolution; it can introduce some efficiencies into the process, but the underlying principles remain the same. Phishing targets or using other social engineering techniques will continue to rely on convincing victims to make poor decisions. The same principles of healthy skepticism and active reporting of suspicious interactions can maintain the security of organizations even with AI-led attacks.

Key Takeaways

✓ **Global threats are on the rise. Organizations of all sizes— but especially critical national infrastructure**—and individuals with access to high-risk information need to look at their defenses, particularly against phishing and similar social engineering attacks.

✓ **Threats powered by AI will continue to rise.** These will prey on humans in the form of social engineering attacks or through disinformation campaigns. Having appropriate knowledge and spreading awareness of the issue is key.

✓ **Some organizations have begun to mature their awareness to work on driving behavior change and building a strong security culture.** These organizations will fare much better in the near future when it comes to reducing risk and having a workforce that makes smarter security decisions.

UK & IRELAND	BASELINE	90 DAYS	1 YEAR
1-249	26.5%	20%	4.1%
250-999	30.2%	21%	4.3%
1000+	35.2%	16.5%	4.8%
Average PPP Across All Organization Sizes	32.3%	18.4%	4.5%

KEY TAKEAWAYS

THE VALUE OF NEW-SCHOOL SECURITY AWARENESS TRAINING

The results from all three phases of the study reveal several conclusions:

- **Every organization is at serious risk without new-school security awareness training.** With an average industry baseline PPP of 34.3%, organizations could be exposed to social engineering and phishing scams by a third of their workforce at any given time.

- **Any organization can strengthen security through end-user training in as little as three months.** The power of a good training program is to set up a consistent cadence of simulated phishing and social engineering education in a rapid timeframe.

- **An effective security awareness training strategy can help accelerate results for all organizations.** The struggle of some enterprise leaders to successfully implement security training effectively across the organization is not surprising. Leaders can set themselves up for success by assessing their goals and plotting an organizational strategy before rolling out training.
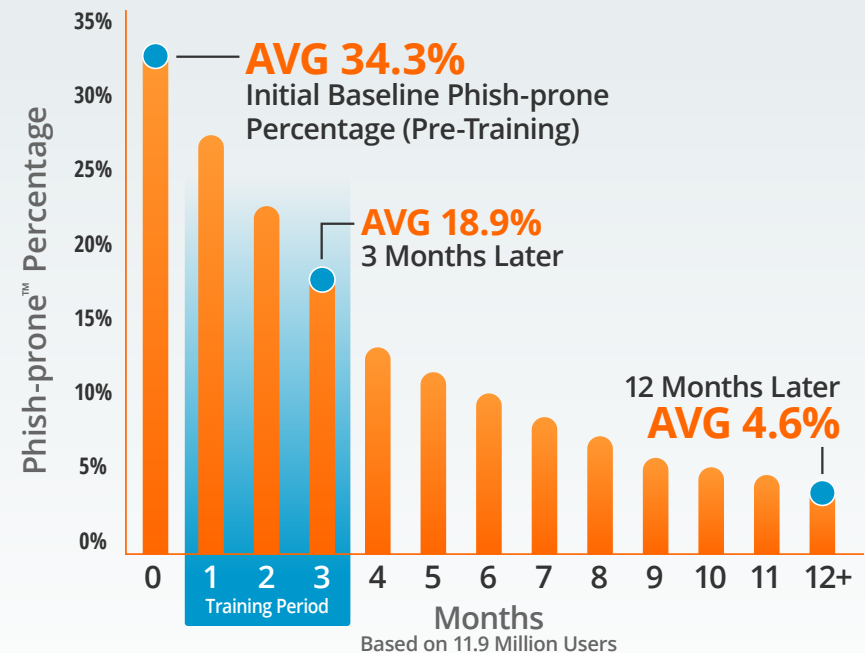
EXECUTIVE TAKEAWAYS

Security and risk management leaders need to understand that in order to favorably change overall security behaviors within their organizations, their programs must have:

- A clearly defined and communicated mandate
- A strong alignment with organizational security policies
- An active connection to overall security culture and human layer of security
- The full support of executives

Without consistent and enthusiastic executive support, raising security awareness within an organization is certain to fail.

Source: 2024 KnowBe4 Phishing by Industry Benchmarking Report

Note: The initial Phish-prone Percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

Chart: Phish-prone™ Percentage vs. Months (0–12+), Training Period at months 1–3.
- AVG 34.3% — Initial Baseline Phish-prone Percentage (Pre-Training)
- AVG 18.9% — 3 Months Later
- 12 Months Later AVG 4.6%
- Based on 11.9 Million Users

SECURITY AND RISK MANAGEMENT EXECUTIVES CAN ENSURE THE SUCCESS OF THEIR PROGRAMS BY:

Fostering a Security Culture

Role Modeling

Engaging a Pro

Thinking Like a Marketer

Mobilizing a Security "Culture Carrier" Program

Adding Ongoing Simulated Phishing Tests

Increasing Frequency

Hiring the Right People

Defining Objectives

Measuring Effectively

Motivating Employees

GETTING STARTED

KnowBe4 is helping tens of thousands of IT pros like you to improve their cybersecurity in fields like finance, energy, healthcare, government, insurance and many more.

With KnowBe4, you have the best-in-class phishing simulation and training platform to improve your organization's last line of defense: **Your Human Firewall**.

We empower your workforce to make smarter security decisions, every day. We help you deliver a data-driven IT security defense plan that starts with the most likely "successful" threats within your organization—your employees. The KnowBe4 methodology really works. Ready to get started?

4 STEPS FOR SAT SUCCESS

It's clear that organizations can radically reduce vulnerability and change end-user behavior through testing and training. Take these steps to get your organization on the right track to developing your human firewall.

1   **Conduct Baseline Testing:** Conducting a baseline test is the first step in demonstrating the need for security awareness training to your senior leadership. This baseline test will assess the Phish-prone Percentage of your users. It's also the necessary data to measure future success.

2   **Train Your Users:** Use on-demand, interactive and engaging computer-based training instead of old-school PowerPoint slides. Awareness modules and videos should educate users on how a phishing or social engineering attempt could happen to them.

3   **Phish Your Users:** At least once a month, test your staff to reinforce the training and continue the learning process. You are trying to train a mindset and create new habits. It takes a while to set that in motion. Simulated social engineering tests at least once a month are effective at changing behavior.

4   **Measure Results:** Track how your workforce responds to both training and phishing. Your goal is to get as close to zero percent PPP as possible.

Learn How To Build A Comprehensive SAT Program

Read Whitepaper →

PLAN LIKE A MARKETER, TEST LIKE AN ATTACKER

While every leader can reduce risk by targeting employee PPP, there are several best practices that can bring about lasting change.

Use real-world attack methods

Your simulated phishing exercises must mimic real attacks and methodologies. Otherwise, your "training" will simply give your organization a false sense of security.

Don't do this alone

Involve other teams and executives, including Human Resources, IT and Compliance teams, and even Marketing. Create a positive, organization-wide culture of security.

Don't try to train on everything

Decide what behaviors you want to shape and then prioritize the top two or three. Focus on modifying those behaviors for 12-18 months.

Make it relevant

People care about things that are meaningful to them. Make sure your simulated attacks impact an employee's day-to-day activities.

Treat your program like a marketing campaign

To strengthen security, you must focus on changing behavior, rather than just telling staff what you'd like them to know. Give them the critical information they need, but stay focused on conditioning their security reflexes so your workforce becomes an effective last line of defense.

CONTRIBUTORS

Anna Collard, Senior Vice President of Content Strategy & Evangelist for KnowBe4 Africa

Megan Colbert, Project Coordinator to the Chief Evangelist & Strategy Officer

Joe Gillet, Director of Sales at KnowBe4

Joanna G. Huisman, Senior Vice President of Strategic Insights and Research at KnowBe4, Lead Author

Erich Kron, Security Awareness Advocate at KnowBe4

Dr. Martin J. Kraemer, Security Awareness Advocate

Javvad Malik, Lead Security Awareness Advocate at KnowBe4 based in London

Jeremy Schwartz, Senior Content Marketing Manager at KnowBe4

Philip Tnee, Senior Director of Sales at KnowBe4

ABOUT KNOWBE4

KnowBe4 empowers your workforce to make smarter security decisions every day. Tens of thousands of organizations worldwide trust the KnowBe4 platform to strengthen their security culture and reduce human risk. KnowBe4 builds a human layer of defense so organizations can fortify user behavior with new-school security awareness and compliance training. Deploying KnowBe4 results in users that are alert and care about the damage that phishing, ransomware and other social engineering threats pose.

The platform includes a comprehensive suite of awareness and compliance training, real-time user coaching, AI-powered simulated social engineering, and crowdsourced anti-phishing defense. With content in 35+ languages, KnowBe4 provides the world's largest, always-fresh library of engaging content to strengthen your human firewall. For more information, please visit www.KnowBe4.com

ADDITIONAL RESOURCES

Free Phishing Security Test
Ready to start phishing your users? Find out what percentage of your employees are Phish-prone with your free phishing security test.

Automated Security Awareness Program
Create a customized Security Awareness Program for your organization.

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click.

Free Email Exposure Check
Find out which of your users emails are exposed before the bad actors do.

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain.

01E05K01